# DESCRIPTION

# INFORMATION PROCESSING DEVICE, INFORMATION RECORDING MEDIUM AND INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM

## Technical Field

[0001]

The present invention relates to an information processing device, information recording medium and information processing method, and computer program, and more particularly relates to an information processing device, information recording medium and information processing method, and computer program which eliminates unauthorized content and realizes strict content usage management, by using an advanced scrambling process for the various content requested of the content usage management.

## Background Art

[0002]

In general, various software data, such as audio data such as music, image data such as movies, game programs, and various application programs (hereafter, referred to as Content) can be stored as digital data in recording media, for example, a Blu-ray disk which uses blue laser, or on a DVD (Digital Versatile Disc), MD (Mini Disc), or CD (Compact Disc). In particular, the Blu-ray disk which uses blue

laser is a disk capable of high density recording, and can record large volumes of movie content and the like as high image quality data.

[0003]

Digital content is stored on such various information recording media (recording media), and is provided to users. A user plays back the content on a playback device such as a PC (Personal Computer) or disk player owned by the user to use the product.

[0004]

Much content such as music data and image data generally has the creator name thereof or distribution rights to the distributor thereof stored therein. Accordingly, generally distribution of such content has certain usage restrictions, this is to say, permission to use the content is granted only for authorized users, and steps are taken so that duplication is not performed without permission.

[0005]

With a digital recording device and recording medium, recording and playback can be performed repeatedly without deterioration in the image or audio thereof for example, and there is a problem of proliferation of unauthorized copied content being distributed via the internet, or so-called pirated disks being shared, where content is copied onto a

CD-R or the like, or copied content is stored on a hard disk such as a PC and used.

[0006]

With a high-capacity recording medium such as a DVD or a recording medium using a blue laser of which development has been advanced in recent years, digital information of a large amount of data such as one to several movies for example can be recorded onto one medium. Thus, as image information and so forth becomes easier to be recorded as digital information, preventing unauthorized copying and protecting the copyrights becomes an increasingly difficult problem. Currently, various technology is in use to prevent unauthorized copying on digital recording devices and recording media, in order to prevent the unauthorized copying of such digital data.

[0007]

For example, with a DVD player, a Content Scramble System is being used. With a Content Scramble System, for example a DVD-ROM (Read Only Memory) has a configuration wherein the video data or audio data is encrypted and recorded, and content playback is performed by reversing the scrambling.

[0008]

With descrambling processing, processing must be executed such as using specified data such as a key provided

to a DVD player which has been granted a license. A license is granted to DVD players which are designed to follow predetermined operation restrictions such as not performing unauthorized copying. Accordingly, with a DVD player which has a license, the specific data such as the provided key is used, and the data recorded on the DVD-ROM is descrambled, and thus images or audio can be played back from the DVD-ROM.

[0009]

On the other hand, a DVD player which does not have a license does not have the specified data such as the key to descramble the scrambled data, and therefore the data recorded onto the DVD-ROM cannot be played back. Thus, with a Content Scramble System configuration, a DVD player which has not satisfied the conditions required at the time of licensing cannot play back the DVD-ROM on which digital data is recorded, and so unauthorized copying is prevented.

[0010]

However, such a Content Scramble System is not necessarily a perfect system, and already descrambling methods are decoded and the decoding methods are often shared via communication means such as the Internet. Thus, once a scramble method is decoded, content is unauthorizedly played back by the unauthorized descrambling processing, and problems arise such as duplications being made and copyrights and utilization rights being infringed.

Disclosure of Invention

Problems to be Solved by the Invention

[0011]

The present invention takes into consideration such situations, and provides an information processing device, information recording medium and information processing method, and computer program which realizes strict content usage management, by setting scrambling processing forms with various differing forms rather than setting uniform processing for scrambling processing of the various content regarding which usage management, such as copyright management, is required, and by executing scrambling processing with a forms being set for each content or each management unit from a large number of scrambling processing forms.

Means for Solving the Problems

[0012]

A first aspect of the present invention is an information recording medium manufacturing method, comprising: a scramble rule acquiring step for acquiring a scramble rule to apply to the content to be recorded on the information recording medium; a scrambling processing step for executing the scrambling processing as to the content, according to the scramble rule acquired in the scramble rule

acquiring step; and a step for recording the scrambled content generated in the scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

[0013]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scramble rule acquiring step is a step for acquiring individual scramble rules for each recording content or for each management unit, in the event of multiple content to be recorded to the information recording medium.

[0014]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scrambling processing step is a step for performing processing to replace at least one portion of the content data to be recorded to the information recording medium; and the scramble rule includes data which points to the position to which the content data is to be replaced.

[0015]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scrambling processing executed in the scrambling processing step is shuffling processing of

shuffle elements which are set as content-comprising data; and the scramble rule is data which describes the shuffle state of the shuffle elements.

[0016]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scrambling processing executed in the scrambling processing step is Exclusive-OR computing processing of the content-comprising data and the previously set settings value or a value calculated based on this settings value; and the scramble rule is data describing the settings value.

[0017]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scrambling processing executed in the scrambling processing step is a rotating processing of the content-comprising data; and the scramble rule is data describing a shift amount in the rotation.

[0018]

Further, an embodiment of the information recording medium manufacturing method according to the present invention further has an encrypting processing step for executing encrypting processing of the recorded content of the information recording medium, after executing the

scrambling processing step, or before executing the same.

[0019]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the scrambling processing executed in the scrambling processing step is a shuffling processing of the shuffled elements which are set as content-comprising data; and the encrypting processing executed in the encrypting processing step is encrypting processing in CBC mode executed on data units the same size as that of the shuffled elements.

[0020]

Further, with an embodiment of the information recording medium manufacturing method according to the present invention, the data for processing which is executed in the scrambling processing in the scrambling processing step is data which includes at least one of the following:

(1) a portion of I-picture slice encoded data included in the MPEG encoded data,

(2) a portion of the sequence header, and

(3) PID data storing the data-type information within the transport stream packet.

[0021]

Further, a second aspect of the present invention is an information processing device for executing content

recording processing as to the information recording medium, comprising: a scrambling processing unit for acquiring a scramble rule to be applied to the content to be recorded on the information recording medium, according to the acquired scramble rule; and a recording processing unit for recording the scrambled content generated in the scrambling processing unit, and the scramble rule applied to this content, to the information recording medium.

[0022]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit has have a configuration for acquiring individual scramble rules for each recording content or for each management unit, in the event of multiple content to be recorded to the information recording medium, and executing scrambling processing for each content according to the acquired scramble rule.

[0023]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit has a configuration for performing processing to replace at least one portion of the content data to be recorded to the information recording medium; and the scramble rule includes data which points to the position to which the content data is to be replaced.

[0024]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing executed in the scrambling processing unit is shuffling processing of shuffle elements which are set as content-comprising data; and the scramble rule is data which describes the shuffle state of the shuffle elements.

[0025]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing executed in the scrambling processing unit is Exclusive-OR computing processing of the content-comprising data and the previously set settings value or a value calculated based on this settings value; and the scramble rule is data describing the settings value.

[0026]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing executed in the scrambling processing unit is a rotating processing of the content-comprising data; and the scramble rule is data describing a shift amount in the rotation.

[0027]

Further, an embodiment of the information processing

device according to the present invention further has an encrypting processing unit for executing encrypting processing of the recorded content of the information recording medium.

[0028]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing executed in the scrambling processing unit is a shuffling processing of the shuffled elements which are set as content-comprising data; and the encrypting processing executed in the encrypting processing unit is encrypting processing in CBC mode executed on data units the same size as that of the shuffled elements.

[0029]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit is data for scrambling processing which includes at least one of the following:

(1) a portion of I-picture slice encoded data included in the MPEG encoded data,

(2) a portion of the sequence header, and

(3) PID data storing the data-type information within the transport stream packet.

[0030]

Further, a third aspect of the present invention is an

information processing device for executing playback processing of the content recorded on the information recording medium, comprising: a scrambling processing unit for executing descrambling processing of the content recorded on the information recording medium; wherein the scrambling processing unit executes analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in the information recording medium, and from the results of the deciphering, executes descrambling processing to the scramble rule for each of the acquired individual content.

[0031]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit has a configuration for acquiring individual scramble rules for each recording content or for each management unit, in the event of multiple content to be recorded to the information recording medium, and executing descrambling processing for each content according to the acquired scramble rule.

[0032]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit has a configuration for performing processing to replace at least one portion of the

content data to be recorded to the information recording medium; and acquires the position data for pointing to the position to which the acquired content data is replaced from the results of analyzing the scramble rule, and based on this position data, executes descrambling processing..

[0033]

Further, with an embodiment of the information processing device according to the present invention, the descrambling processing executed with the scrambling processing unit is processing for restoring the shuffle state of the shuffle elements which are set as content-comprising data; the scramble rule is data describing the shuffle state of the shuffle elements; and the scramble processing unit executes shuffle state restoring processing of the shuffle elements based on the scramble rule.

[0034]

Further, with an embodiment of the information processing device according to the present invention, the descrambling processing executed with the scrambling processing unit is Exclusive-OR computing processing of the content-comprising data and the previously set settings value or a value calculated based on this settings value; the scramble rule is data describing the settings value; and the scramble processing unit executes Exclusive-OR computing processing of the content-comprising data and the previously

set settings value based on the scramble rule.

[0035]

Further, with an embodiment of the information processing device according to the present invention, the descrambling processing executed with the scrambling processing unit is rotation processing for the content-comprising data; the scramble rule is data describing the shift amount in the rotation; and the scramble processing unit executes rotation restoring processing based on the shift amount, based on the scramble rule.

[0036]

Further, with an embodiment of the information processing device according to the present invention, the information processing device further comprises an encrypting processing unit for executing decrypting processing of the recorded content of the information recording medium.

[0037]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing executed in the scrambling processing units is shuffling processing of the shuffle elements which are set as content-comprising data; and the decrypting processing executed in the encrypting processing units is decrypting processing in CBC mode executed on data units the

same size as that of the shuffled elements.

[0038]

Further, with an embodiment of the information processing device according to the present invention, the scrambling processing unit is data for descrambling processing which acquires data including at least one of the following and executing processing thereof:

(1) a portion of I-picture slice encoded data included in the MPEG encoded data,

(2) a portion of the sequence header, and

(3) PID data storing the data-type information within the transport stream packet.

[0039]

Further, a fourth aspect of the present invention is an information recording medium for storing recorded data as scrambled content having scrambling processing executed according to a scramble rule set for each recording content or for every management unit; and the scramble rule applied to the scrambled content.

[0040]

Further, with an embodiment of the information recording medium according to the present invention, the scrambling processing is processing for replacing at least one portion of the content; and the scramble rule is a rule for recording the data showing the position of the portion

of data of the content data to be replaced.

[0041]

Further, with an embodiment of the information recording medium according to the present invention, the scrambled content is scrambled content generated by the shuffling processing of the shuffle element set as the content-comprising data; and the scramble rule is data describing the shuffle state of the shuffle elements.

[0042]

Further, with an embodiment of the information recording medium according to the present invention, the scrambled content is scrambled content generated by Exclusive-OR computing processing of the content-comprising data and the previously set settings value or a value calculated based on this settings value; and the scramble rule is data describing the settings value.

[0043]

Further, with an embodiment of the information recording medium according to the present invention, the scrambled content is scrambled content generated by rotation processing of the content-comprising data; and the scramble rule is data describing a shift amount in the rotation.

[0044]

Further, with an embodiment of the information recording medium according to the present invention, the

scrambled content is scrambled content generated by shuffling processing of the shuffle elements which as set as content-comprising data; and the information recording medium has the configuration to record content encrypted by the encrypting processing in CBC mode which executes with data the same size as that of the shuffled elements as a unit.

[0045]

Further, with an embodiment of the information recording medium according to the present invention, having a configuration wherein the scrambled content includes as scrambling processing data at least one of the following:

(1) a portion of I-picture slice encoded data included in the MPEG encoded data,

(2) a portion of the sequence header, and

(3) PID data storing the data-type information within the transport stream packet.

[0046]

Further, a fifth aspect of the present invention is an information processing method for executing content recording processing to an information recording medium, comprising: a scramble rule acquiring step for acquiring a scramble rule to apply to the content to be recorded on the information recording medium; a scrambling processing step for executing the scrambling processing as to the content,

according to the scramble rule acquired in the scramble rule acquiring step; and a step for recording the scrambled content generated in the scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

[0047]

Further, a sixth aspect of the present invention is an information processing method for executing playback processing of the content recorded on an information recording medium, comprising: a scrambling processing step for executing descrambling processing of the content recorded on the information recording medium; wherein the scrambling processing step further comprises a scramble rule analyzing step for executing analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in the information recording medium, and a descrambling step for, based on the results of the scramble rule analyzing step, executing descrambling processing corresponding to the scramble rule for the acquired individual content.

[0048]

Further, a seventh aspect of the present invention is a computer program for executing content recording processing to an information recording medium with a computer, comprising: a scramble rule acquiring step for acquiring a

scramble rule to apply to the content to be recorded on the information recording medium; a scrambling processing step for executing the scrambling processing as to the content, according to the scramble rule acquired in the scramble rule acquiring step; and a step for recording the scrambled content generated in the scrambling processing step and the scramble rule applied to the content, onto an information recording medium.

[0049]

Further, an eighth aspect of the present invention is a computer program for executing playback processing of the content recorded on the information recording medium with a computer, comprising: a scrambling processing step for executing descrambling processing of the content recorded on the information recording medium; wherein the scrambling processing step further comprises a scramble rule analyzing step for executing analyzing of the scramble rule which is the scrambling processing information corresponding to the content stored in the information recording medium, and a descrambling step for, based on the results of the scramble rule analyzing step, executing descrambling processing corresponding to the scramble rule for the acquired individual content.

[0050]

The computer program according to the present invention

is, for example, a computer program which can provide a computer system which can execute various program codes with a memory medium, communication media, recording media such as CD, FD, or MO, or a communication medium such as a network, in a computer-readable format. By providing such a program in a computer-readable format, processing according to the program can be realized with the computer system.

[0051]

Further objects, features, and advantages of the present invention will become apparent through the detailed descriptions based on the below-described embodiments of the present invention or the attached diagrams thereof. In this specification, a system is considered to be the configuration of a logical collection of multiple devices, and does not limit the devices for each configuration to be housed within one unit.

Advantages

[0052]

With the configuration according to the present invention, the scrambling processing forms with various differing forms are set, rather than setting uniform processing for scrambling processing of the various content as requested by the usage management system such as copyright management, and scrambling processing is executed with a form being set for each content or each management

unit from a large number of scrambling processing forms, and therefore, if by chance there is an event wherein scrambling for a given content is unauthorizedly decoded and the content is leaked, the content which has a scrambling process with a different scrambling form cannot be descrambled, and so leakage of content can be kept to a minimum.

[0053]

With the configuration according to the present invention, scrambling processes such as shuffling processing, EXOR processing, and rotation processing are executed, and with shuffling processing, various shuffle forms are specified as the scramble rules, and with EXOR processing, values applicable to EXOR are specified as the scramble rules, and with rotation processing, the rotation shift amounts are specified as the scramble rules. For example, in the case of using 32 shuffle elements with shuffling processing, 32! different shuffle forms, that is to say, scramble rules, can be specified. Also, with EXOR processing, the values applicable to EXOR, and with rotation processing, various values of the shift amount, can be set, and so a large number of scramble rules can be set, so a configuration is realized wherein scrambling of each content based on the rules selected from this large number of scramble rules is performed, and based on the leakage of

specified scramble rules, leakage of a large amount of content can be prevented.

## Brief Description of the Drawings

[0054]

Fig. 1 is a diagram describing a storage data configuration of an information recording medium, and the configuration and processing of an information processing device which executes playback processing.

Fig. 2 is a diagram describing a settings example of a content management unit for setting the storage content of the information recording medium.

Fig. 3 is a diagram showing corresponding examples of the content management unit configuration and a scramble rule.

Fig. 4 is a diagram describing the content playback sequence in an information processing device which executes content playback.

Fig. 5 is a diagram describing details of encrypting processing such as key generating which is used for content playback in the information processing device.

Fig. 6 is a flowchart describing content playback order in an information processing device which executes content playback.

Fig. 7 is a diagram describing processing for executing

a licensing entity, authoring facility, and encrypting facility.

Fig. 8 is a diagram describing content data transition in the event of executing shuffle processing as the scrambling processing.

Fig. 9 is a diagram describing a scramble rule in the event of executing shuffle processing as the scrambling processing.

Fig. 10 is a diagram describing the details of encrypting processing in the event that content encrypting is executed with a 6 KB Aligned Unit as a unit.

Fig. 11 is a diagram describing the details of encrypting processing using AES_ECBC mode.

Fig. 12 is a diagram describing the details of encrypting processing in the event that content encrypting is executed with 2 KB User Sector Data as a unit.

Fig. 13 is a diagram describing a help file to be used when executing content encrypting.

Fig. 14 is a diagram showing the help file syntax to be used when executing content encrypting.

Fig. 15 is a diagram describing processing for executing a licensing entity, authoring facility, and encrypting facility in the event of executing scrambling processing with the encrypting facility.

Fig. 16 is a diagram describing content data transition

in the event of executing shuffle processing as the scrambling processing in the event of executing scrambling processing with the encrypting facility.

Fig. 17 is a diagram describing the configuration of MPEG-2 transport stream data.

Fig. 18 is a diagram describing the syntax of a source packet and header comprising the MPEG-2 transport stream data.

Fig. 19 is a diagram describing the syntax of a transport packet comprising the MPEG-2 transport stream data.

Fig. 20 is a diagram describing content data transition in the event of executing Exclusive-OR (EXOR) processing as the scrambling processing.

Fig. 21 is a diagram describing the scramble rule in the event of executing Exclusive-OR (EXOR) processing as the scrambling processing.

Fig. 22 is a diagram describing an EP map which can be used for acquiring a position of an I-picture for example which comprises the MPEG data.

Fig. 23 is a diagram describing an EP map which can be used for acquiring a position of an I-picture for example which comprises the MPEG data.

Fig. 24 is a diagram describing a processing example in the event of executing Exclusive-OR (EXOR) processing as the scrambling processing as to a slice of an I-picture.

Fig. 25 is a diagram describing a processing example in the event of executing Exclusive-OR (EXOR) processing as the scrambling processing as to a sequence header.

Fig. 26 is a diagram describing content data transition in the event of executing Exclusive-OR (EXOR) processing as the scrambling processing in the event of executing scrambling processing with the encrypting facility.

Fig. 27 is a diagram describing content data transition in the event of executing rotation processing as the scrambling processing.

Fig. 28 is a diagram describing a scramble rule in the event of executing rotation processing as the scrambling processing.

Fig. 29 is a diagram describing content data transition in the event of executing rotation processing as the scrambling processing in the event of executing scrambling processing with the encrypting facility.

Fig. 30 is a diagram describing a configuration example of an information processing device for recording information or executing playback processing as to the information recording medium.

## Best Mode for Carrying Out the Invention

[0055]

Hereafter, the details of an information processing

device, information recording medium and information processing method, and computer program will be described with reference to the diagrams. It should be noted that the descriptions will follow the itemized list as follows.

1. Storage data and playback processing of the information recording medium

2. Details of content recording processing of the information recording medium

(2-1) Shuffling processing

(2-2) Exclusive-OR (EXOR) processing

(2-3) Rotating processing

3. Configuration examples of the information processing device.

[0056]

[1. Storage data and playback processing of the information recording medium]

First, content playback processing with the storage data of the information recording medium and the information processing device (playback device) will be described. Fig. 1 shows a configuration of an information recording medium 100 wherein content is stored which can be processed according to the present invention, and an information processing device (playback device) 150. Here, an information storage example of a ROM disk is shown as a disk on which content is already stored. The information

processing device (playback device) 150 can be various information processing devices, such as a PC for example or a device specifically for playing back, and has a drive 120 which executes data reading processing for the information recording medium 100.

[0057]

The ROM disk which is the information recording medium 100 is an information recording medium such as a Blu-ray disk or DVD for example, and is an information recording medium storing legal contents which has been manufactured in a disk manufacturing plant under the authority of so-called content right-holder having legal content copyrights or distribution rights. With the embodiments below, the example of a disk-type medium is described as an example of the information recording medium, but the present invention is applicable to information recording mediums of various forms.

[0058]

As shown in Fig. 1, the information recording medium 100 comprises encrypted content 111 having scrambling processing and encrypting processing performed; an MKB (Media Key Block) 112 as an encryption key block generated based on a key distribution method of a tree structure which is known as a form of a broadcast encryption method; a volume ID 113 which is set as identifying information for

individual information recording mediums or for each information recording medium in a unit of a predetermined number of disks, licensing information 114 which includes CCI (Copy Control Information) as the content copy/playback control information; title key data 115 which comprises a recording seed (REC SEED) as necessary information for generating a title key to use in content decrypting processing; and further, scramble rules 116 storing information as to form of scrambling processing has been performed for each content stored in the information recording medium 100 or management unit thereof.

Now, an outline of the various types of information will be described.

[0059]

(1) Encrypted content 111

Various content is stored in the information recording medium 100. This is content such as game programs, image files, audio data, or text data in forms regulated by specified standards or AV(Audio Visual) streaming of moving image content such as HD (High Definition) movie content which is high resolution moving image data, for example. This content is specified AV format standard data, and is stored according to specified AV data formatting. Specifically, for example Blu-ray disk ROM regulation data is stored according to Blu-ray disk ROM regulation

formatting. This is called the main content.

[0060]

Further, game programs, image files, audio data, or text data, for example, may be stored as sub-content as extra (service) data. The sub-content is data having a data format which does not follow the specified AV data formatting. In other words, this can be stored with any formatting without following Blu-ray disk ROM regulation formatting as Blu-ray disk ROM non-standard data,. This is called the sub-content.

[0061]

Types of content for both main content and sub-content include various content such as music data, moving images, image data of still images, game programs, and WEB content, and this content includes various forms of information such as content information usable only by data from the information recording medium 100, content information usable by data from the information recording medium 100 together with data provided from a server which is connected to a network. The content stored in an information recording medium is divided by content section and different keys (title keys) assigned and encrypted and stored, so as to realize usage control differing for each section of content. A unit to which one title key is assigned is called a content management unit (CPS unit).

[0062]

(2) MKB

The MKB (Media Key Block) 112 is an encryption key block generated based on a key distribution method of a tree structure which is known as a form of a broadcast encryption method. MKB 111 is a key information block which is able to acquire a media key (Km) which is a key necessary for content decrypting, only by processing (decrypting) based on a device key stored in the information processing device of a user with a valid license. This key can be acquired only in the case that the user device (information processing device) has a valid license, by an information distribution method according to a so-called hierarchy tree structure, and the acquiring of a key (media key) of a user device which has been invalidated (revoking processing) can be stopped. With the changes to the key information stored in the MKB, the management center can generate a MKB with a configuration which cannot decrypt with the specified device key stored in the user device, that is to say, cannot acquire the media key necessary for content decrypting. Accordingly, unauthorized devices can be eliminated (revoked) at arbitrary timing, and thus encrypted content can be provided which can only be decrypted by devices with a valid license. The decrypting process of content will be described later.

[0063]

(3) Volume ID

The volume ID is an ID which is set as identifying information for each information recording medium within a unit made up of a predetermined number of disks, or for individual information recording media. This volume ID is used as title key generating information to be used in the decrypting of the content. This processing will be described later.

[0064]

(4) Licensing information

Licensing information includes, for example, copy/playback control information (CCI). This is copy restriction information or playback restriction information for usage control corresponding to the encrypted content 111 stored in the information recording medium 100. This copy/playback control information (CCI) can have various settings, such as the case of setting information for individual CPS units which as set as content management units, or the case or setting corresponding to multiple CPS units. The details of this information will be described later.

[0065]

(5) Title key data

As described above, each content or collection of

multiple content is encrypted using individual encryption keys (title keys) for each, for content usage management, and is stored in the information recording medium 100. That is to say, it becomes necessary for the AV(Audio Visual) stream, music data, moving images, image data of still images and the like, game programs, WEB content, and so forth which comprise the content, to be divided into units of content usage management units, different title keys to be generated for each divided unit, and decrypting processing to be performed. The information for generating this title key is the title key data, and a recording seed comprising a portion of data of the content is used, for example.

[0066]

Title keys corresponding to each unit are generated according to a predetermined encrypting key generating sequence using the title key data 115, and content decrypting is executed.

[0067]

(6) Scramble rule

As described above, the content stored in the information recording medium 100 has encrypting processing performed, and further has scrambling processing performed. The scrambling processing is executed with different forms for each content or content management unit (CPS unit)

stored in the information recording medium 100. Accordingly, when performing content playback, the scrambling processing information performed on the content for playback is acquired, and descrambling processing must be performed corresponding to the executed scrambling processing. The scramble rule 116 is recorded data of the scramble form information for each content or content management unit (CPS unit) stored in the recording information recording medium 100. This scramble rule is recorded in the information medium as data which is decodable only in an information processing device which has a license. The data is recorded using a secure code for example, Java secure code for example, and so decoding can only be performed with secure code decoding processing within a Java virtual machine which is set in the playback device.

[0068]

Fig. 1 shows an outline of the configuration of the information processing device 150 which executes playback processing of the content stored in the information recording medium 100. The information processing device has a drive 120 which executes reading processing of the stored data in the information recording medium. The data read by the drive 120 is input into a playback processing executing LSI 151 which executes decrypting processing and decoding processing (for example MPEG decoding) of the encrypted

content.

[0069]

The playback processing executing LSI 151 has a decrypting processing unit 152 for executing decrypting processing of the encrypting content, and a decoding processing unit 153 for executing decoding (for example MPEG decoding) processing. With the decoding processing unit 152, a title key is generated from a device key stored in the memory 155 and the reading data from the information recording medium 120, and decrypting processing of the encrypting content 111 is executed.

[0070]

The decrypted content has scrambling processing executed therein. An descrambling executing unit 154 executes this descrambling. After the decrypted content has the descrambling processing executed thereupon which is determined based on the scramble rule 115, with the descrambling executing unit 154, the descrambled data is input again into the playback processing executing LSI 151, and decoding processing is executed in the decoding processing unit 153, and the data is output and played back. The details of the content decrypting and descrambling processing sequence in the information processing device 150 will be described later.

[0071]

Next, the content management configuration which divides the content stored in the information recording medium and realizes usage control that differs for each divided content will be described with reference to Fig. 2 and subsequent drawings.

[0072]

As described above, the content stored in an information recording medium is divided by content section, assigned different keys (title keys) for each divided content, encrypted, and further scrambled and stored, so as to realize usage control differing for each section of content. A unit to which one title key is assigned is called a content management unit (CPS unit).

[0073]

Content belonging to each unit is encrypted applying the respective title keys, and at the time of content usage, a key (title key) assigned to each unit is acquired, and further descrambling corresponding to the scramble rules is executed and playback is performed. Each title key can be managed individually, and for example a title key assigned to a unit A can be set as a key which can be acquired from the information recording medium. Also, a title key assigned to unit B can be acquired under the condition that the server connected to the network is accessed and the user has executed predetermined requirements, and so acquiring

keys corresponding to the various units and the management configuration thereof can be set independently for the various title keys.

[0074]

A settings form of the unit to which one key is assigned, that is to say, a content management unit (CPS unit) will be described with reference to Fig. 2.

[0075]

As shown in Fig. 2, the content has a hierarchical structure with (A) a title 210, (B) a movie object 220, (C) a playlist 230, and (D) a clip 240, and when the title is specified which is an index file accessed by the playback application, the playback program associated with the title is specified, a playlist is selected which has the content playback order and so forth regulated according to the program information of the specified playback program, then an AV stream or command as the content actual data is read out by the clip information which is regulated in the playlist, and playback of the AV stream or executing processing of the command is performed.

[0076]

Fig. 2 shows two CPS units. These configure a portion of the content stored in the information recording medium. Each of the CPS unit 1 and 271 and CPS unit 2 and 272 are CPS units which are set as units including the title as an

application index, and a movie object as a playback program file, and a playlist, and a clip which includes an AV stream file as content actual data.

[0077]

The content management units (CPS units) 1 and 271 contain titles 1 and 211 and titles 2 and 212, playback programs 221 and 222, playlists 231 and 232, and clip 241 and clip 242; and the AV stream data files 261 and 262, which are the actual data of the content contained in these two clips 241 and 242, are encrypted using the title key: Ku1 which is the encryption key which is set corresponding to the content management units (CPS unit) 1 and 271.

[0078]

The content management units (CPS units) 2 and 272 contain titles 3 and 213, playback program 224, playlist 233, and clip 243; and the AV stream data file 263, which is the actual data of the content contained in the clip 243, is encrypted using the title key: Ku2 which is the encryption key which is set corresponding to the content management units (CPS unit) 2 and 272.

[0079]

For example, in order for the user to execute an application file or content playback process corresponding to the content management units 1 and 271, the title key: Ku1, which is the encryption key and which is set

corresponding to the content management units (CPS units) 1 and 271, must be acquired, and decrypting processing must be executed, and after executing the decrypting processing, the application program can be executed and the content can be played back. In order to execute an application file or content playback process corresponding to the content management units 2 and 272, the title key: Ku2, which is the encryption key and which is set corresponding to the content management units (CPS units) 2 and 272, must be acquired, and decrypting processing must be executed.

[0080]

With the scrambling processing also the same applies, and scrambling processing which differs for each content management unit is executed and stored in the information recording medium. For example, scrambling processing using scramble rule #1 is performed as to the CPS units 1 and 271, and scrambling processing using scramble rule #1 is performed as to the CPS units 2 and 272. For descrambling at the time of content playback, the descrambling process corresponding to each scramble rule must be executed. The scramble rule can also have a form such as changing with the content contained in the CPS unit.

[0081]

Fig. 3 is a table showing the correlation between each content and CPS unit and scramble rule in the case that

different scramble rules are used for each CPS unit. As shown in Fig. 3, the content management unit (CPS unit) corresponding to the index or application file of the application layer or data group and the scramble rules are correlated.

[0082]

The information processing device 150 which executes content playback processing identifies the content management unit (CPS unit) for playing back, and from the scramble rules 116 acquires the scramble rule which is executed as to the content management unit for playing back, and descrambling processing is executed corresponding to the applicable rule, thus executing the descrambling.

[0083]

With the configuration of the present invention, the scrambling processing which is used for the content stored in the information recording medium are not identical, but rather is a form wherein the scrambling processing is different for each individual content management units (CPS units) or content; and for playback processing, descrambling processing must be executed corresponding to the scramble rule applicable as to each content management unit (CPS units) or content.

[0084]

Next, with reference to Fig. 4, details will be

described of the content playback processing in the information processing device which acquires content from the information recording medium wherein the encrypted content, which has had encryption at the CPS unit level and scrambling processing as described above, and various key generating information and the scramble rules are stored, and which executes playback processing.

[0085]

As shown in Fig. 4, the content playback processing which is executed in the information processing device 150 contains the two processes which are the decrypting processing of the encrypted content and the descrambling processing.

[0086]

The information processing device 150 reads the various information from the information recording medium 100, and decrypting processing of the encrypted content is executed based on the title key generated by the key generating processing which uses readout data and the device key 301 kept by the information processing device 150, and further, descrambling processing of the decrypted content is executed. With this embodiment, an example is shown wherein descrambling is performed after the decrypting processing of the content, but there can be a configuration for performing decrypting processing after the descrambling processing, and

this processing sequence is dependent on the recording processing sequence of the content stored in the information recording medium.

[0087]

The detailed sequences of the decrypting process and the descrambling process of the encrypted content in the information processing device 150 will be described with reference to Fig. 4. With the content decrypting process, first, the information processing device 150 reads out the device key 301 stored in the memory. The device key 301 is a secret key stored in the information processing device which has received a license related to use of the content.

[0088]

Next, in step S11, the information processing device 150 executes decrypting processing of the MKB 112 which is the encryption key block wherein is stored the media key Km stored in the information recording medium 100, using the device key 301, and acquires the media key Km.

[0089]

Next, in step S12 a title generating key Ke (embedded Key) is generated by the encrypting processing based on the media key Km acquired in the MKB processing in step S11, and the volume ID 113 read out from the information recording medium 100. This key generating process is executed as processing according to for example an AES encryption

algorithm.

[0090]

The details of the AES encryption algorithm will be described with reference to Fig. 5. An example of a process according to the AES encryption algorithm is applying an AES-based hash function [AES_H]. The AES-based hash function is configured by a combination of the Key Generation processing executing unit (AES_G) accompanying the data decrypting processing using the AES encryption processing, and EXOR unit. The AES_G portion is configured of the combination of the AES decryption unit (AES_D) and the EXOR unit, as Fig. 5 further shows.

[0091]

The generating process for the title key generating key Ke (embedded Key) in step S12 in Fig. 4 takes as input the media key Km acquired in the MKB process in step S11 and the volume ID 113 read out from the information recording medium 100, and executes the hash function of the AES base [AES_H] shown in Fig. 5 for example.

[0092]

Next, in step S13, a control key Kc is generated by the encryption processing (AES_H) based on the title key generating key Ke (embedded Key) and the licensing information 114 read out from the information recording medium 100, and in step S14, the title key is generated by

the encryption processing (AES_H) based on the control key Kc and the title key data 115 which is read out from the information recording medium 100.

[0093]

Next, in step S15, decrypting processing (for example AES_D) using the title key is executed as to the encrypted content read out from the information recording medium 100.

[0094]

Next, in step S16, descrambling processing of the decrypted content is executed. The descrambling process of the step S16 comprises a scramble rule acquiring process in step S16a and a descrambling process in step S16b.

[0095]

As described above, the content has scrambling processing performed thereto with the applicable scramble rule which differs for each content management unit or each content, and is stored in the information recording medium 100. The scramble rule acquiring process in step S16a is processing which acquires the scramble rule 115 stored in the information recording medium 100 and deciphers the scramble rule corresponding to the content for playback. The descrambling processing in step S16b executes the descrambling process which corresponds to the scramble rule deciphered in step S16a.

[0096]

The scramble rule acquiring step in S16a and the descrambling process in step S16b must be executed as secure data processing so that the scramble rule does not leak. The scramble rule 115 stored in the information recording medium is determined with a secure Java code, and the information processing device 150 executes the scramble rule acquiring process in step S16a and the descrambling process in step S16b as the processing within the Java virtual machine which Java realizes.

[0097]

After this, decoding processing such as MPEG decoding, for example, is executed in step S17 to the content data after the descrambling, and the content 302 is output.

[0098]

The content playback sequence which is executed by the information processing device 150 will be described with reference to the flowchart shown in Fig. 6. In step S101, the decrypting processing of the MKB 112 stored in the information recording medium 100 is executed with the applicable device key, and the media key Km acquiring processing is executed. In step S102, in the event that the acquiring of the media key is determined to be a success, the flow continues to step S103.

[0099]

In Step S102, in the case that the acquiring of the

media key is determined to be a failure, the flow continues to step S109, playback is prohibited, and the process ends. The case in which the acquiring of the media key fails refers to the state in which the device key maintained by the information processing device is revoked, that is to say the license is not recognized. As described above, the MKB can be configured to be updated as necessary, and the media key is able to be acquired only when the storage device key is used in an information processing device which maintains a valid license, and in the case it is revoked, the media key cannot be acquired.

[0100]

In the case that the acquiring of the media key succeeds, the flow proceeds to step S103, and the title key generating key Ke (embedded Key) is generated by the encrypting process based on the acquired media key Km and the volume ID 113 read out from the information recording medium 100. This key generating process is executed as a process using an AES-based hash function [AES_H] as shown in Fig. 5 for example, as described above.

[0101]

Next, in step S104, the control key Kc is generated by the encryption process (AES_H) based on the title key generating key Ke (embedded Key) and the license information 114 read out from the information recording medium 100, and

in step S105, the title key is generated by the encryption process (AES_H) based on the control key Kc and the title key data 115 read out from the information recording medium 100.

[0102]

Next, in step S106, decrypting processing (for example AES_D) using the title key is executed as to the encrypted content read out from the information recording medium 100, and in step S107, the scramble rule 115 stored in the information recording medium 100 is acquired, and the processing for deciphering the scramble rule corresponding to the content to be played back is executed, and in step S108, the descrambling processing corresponding to the descrambled rule is executed.

[0103]

[2. Details of content recording processing of the information recording medium]

Next, the details of the content recording process as to the information recording medium will be described. The manufacturing sequence of the content storage information recording medium will be described, with reference to Fig. 7.

[0104]

As shown in Fig. 7, first, for the content stored in the information recording medium, editing processing in an authoring facility 330 which executes content editing

processing, that is to say, authorizing processing is executed in step S201, and the authorized content 332 is generated. The authoring content is normally set as content which has been encoded with an MPEG encoding or the like.

[0105]

Further, an applicable scramble rule 331 is selected, and based on the selected scramble rule, scrambling processing is executed in step S202. It should be noted that there are various forms of the scrambling forms. These specific forms will be described later. In Step S202, after the scrambling processing is performed, the scrambled content is transferred to the encryption facility 370 which serves as a disk plant for executing information recording medium manufacturing processing.

[0106]

With the encryption facility 370, in step S203, encryption processing is executed as to the scrambled content. A licensed entity 350 executes the management of the MKB which is an encryption key block as described above, and provides the media key Km to the encryption facility 370 which executes content encryption processing, and the encryption facility 370 executes processing using the media key, and executes content encryption. The details of the encryption process will be described later.

[0107]

The encrypted content 371 which is generated by the encryption processing in step S203 and the scramble rule 331 used in the authoring facility 330 are written in to the information recording medium 100 with the encryption facility 370, and the information recording medium 100 is manufactured.

[0108]

As examples of the scrambling processing, the three types of scrambling processing below will be described in order.

(2-1) Shuffling processing

(2-2) Exclusive-OR (EXOR) processing

(2-3) Rotation processing

[0109]

[(2-1) Shuffling processing]

Fig. 8 is a diagram showing the generating processing of the recorded data described in Fig. 7 as modified content data, and shows a processing example in the case of using shuffling processing as the applicable scrambling processing. In the case of using shuffling processing as the scrambling processing, various different shuffle forms can be set for each scramble rule. That is to say, a large number of shuffle forms can be set as follows:

Scramble rule #1: Shuffle form 1

Scramble rule #2: Shuffle form 2

Scramble rule #3: Shuffle form 3

: : :

Scramble rule #n: Shuffle form n

and one of the scramble rules #x (shuffle form x) is used for each content or each content management unit (CPS unit), and scrambling processing is thus executed.

[0110]

Fig. 8 shows, from the top layer, (A) plaintext before shuffling processing, plaintext after shuffling processing, and (C) shuffled encrypted text. As shown in Fig. 8(A), the content which is encoded with MPEG encoding or the like, that is to say, the content such as an AV stream recorded onto the information recording medium, is divided from the head into 64 KB each, and is set with a shuffle unit for every 64 KB. The 64 KB shuffle units comprise thirty-two 2 KB shuffle elements.

[0111]

The shuffling processing as the scrambling processing is executed as interchange (shuffling) of the 2 KB shuffle elements. The shuffle form as an interchange form is the scramble rule. The scramble rule (shuffle form) will be described with reference to Fig. 9. Fig. 9 (A) shows an example of one scramble rule (shuffle form).

[0112]

The scramble rule (shuffle form) shown in Fig. 9 (A)

shows the reordering (reordered positions) by shuffling the 2 KB shuffle elements 1 through 32 shown in Fig. 8. In other words with this shuffle rule, after shuffling, the third shuffle element before shuffling is set as the first shuffle element, and the nineteenth shuffle element before shuffling is set as the second shuffle element, and thereafter similarly, the shuffling processing reorders the shuffle elements as 16, 24, 26….

[0113]

Fig. 9 (B1) is the set sequence of the 2 KB shuffle elements 1 through 32 before shuffling, and (B2) is the set sequence of the 2 KB shuffle elements 1 through 32 after shuffling which is generated by the scrambling processing used in the scramble rule (shuffle form) in (A).

[0114]

As described above, the scramble rule (shuffle form) can be set as different rules for each content or content management unit (CPS unit). In the event that multiple content or content management units (CPS units) are recorded on the information recording medium, the scramble rules which are used corresponding to each content or content management unit (CPS unit), that is to say, for example the scramble rules shown in Fig. 9(A) are each recorded as the scramble rule 116 described with reference to Fig. 1. The information processing device which executes the playback

processing reads out the scramble rules corresponding to the content to be played back, and executes descrambling processing.

[0115]

The example shown in Fig. 8 and Fig. 9 is an example wherein shuffling using 32 shuffle units is executed as the scrambling processing. In this event, there are 32! types of settings of shuffle forms, and so 32! rules can be set as the scramble rules. Scrambling processing can be executed by applying one of these 32! rules to each content or content management unit (CPS unit). Accordingly, even in the event that a scramble rule set for one content is leaked, the probability that the scramble rules used for the other contents being the same scramble rule is extremely small, and so descrambling the other content based on the leaked scramble rule is almost impossible, and thus can prevent unauthorized acquiring and use of the content.

[0116]

The scramble rule 116 which is recorded on the information recording medium is described in encrypted data, for example Java secure code, and is set as data readable only by an information processing device holding a valid license, and so unauthorized rule decoding and reading is prevented.

[0117]

The scrambling processing (shuffling processing) can be set to execute for all of the multiple 64 KB shuffle units which are set by dividing the content, but can also be set to execute scrambling (shuffling) processing for only a portion of the units which is selected from the multiple 64 KB shuffle units which are set by dividing the content.

[0118]

The above-described example is shown with the shuffle unit being set as 64 KB, but the data size is not limited to this. However, by having the shuffle unit size the same size as the size of the ECC block which is set as a data readout unit of the drive in the content playback processing in the information processing device, which is 64 KB, the shuffled units can be read by taking one data reading. Accordingly, by setting the shuffle units to 64 KB, the deshuffle processing and the data acquiring processing which is executed in the drive at the time of playback processing can be executed as one set of processing, and efficient processing can be realized. Also, as will be described later with reference to Fig. 17, a transport packet which uses a 192 byte unit as a logical unit is used for recording, and thus processing can be performed with this unit, and further only one portion of this transport packet can have the shuffling processing performed. Also, dummy data can be inserted, and reordered with the scramble rule shown in Fig.

9 such that the dummy data is removed.

[0119]

Also, the size = 2 KB of the shuffle elements is the same size as the user sector data of a Blu-ray disk. With an Aligned Unit which is set with a 6 KB unit, only the first 16 bytes are set as un-encrypted data (plaintext), as shown in Fig. 8. At the head of each Aligned Unit (6 KB), a time stamp is set as the playback processing timing information.

[0120]

With the content encryption processing to be described later, in the case of executing encryption processing with 6 KB units, by executing a shuffle with 2 KB units, it is more likely for time stamp information to be included in either the second or third user sector data of each Aligned Unit (6 KB), but this information is to be encrypted. Thus, by encrypting much of the time stamp information, acquiring the playback sequence based on the time stamp information is impossible unless correct decrypting processing and unscrambling processing is not executed.

[0121]

As shown in Fig. 8 (A) and (B), for example the scrambling processing (shuffling processing) using the scramble rule shown in Fig. 9 is executed in an authoring facility, and the shuffled data is transferred to a disk

plant as an encryption facility and encryption processing is executed, and the shuffled encrypted text shown in Fig. 8(C) is generated.

[0122]

As a form of the encryption processing, for example, there is a setting using a 6 KB Aligned Unit (6 KB) as the encryption processing unit and a setting using a 2 KB user sector data as the encryption processing unit, and each of these encryption processing forms will be described below.

[0123]

First, the encryption processing using the setting using a 6 KB Aligned Unit (6 KB) as the encryption processing unit will be described with reference to Fig. 10.

[0124]

Fig. 10(A) shows a data configuration the shuffled plaintext set as a 6 KB unit Aligned Unit. Each 6 KB Aligned Unit is set as a group of three 2 KB user sector data, as shown in Fig. 10(B).

[0125]

The encryption processing is executed using AES_ECBC, that is to say, a CBC (Cipher Block Chaining) mode of AES encryption, with the 6 KB Aligned unit, which is formed of three 2 KB user sector data, as a processing unit. The key to use for encryption processing is the block key (128 bits) generated by the AES key generating processing from the

placement EXOR and AES encryption based on the above-described title key (128 bits), and the block key generating data acquired from the first 16B un-encrypted portion 401 of the 6 KB Aligned Units. The block key is generated using the block key generating data acquired from the first 16B un-encrypted portion 401 of the 6 KB Aligned Units, and so a different key is set for each 6 KB Aligned Unit.

[0126]

The encryption processing in AES_ECBC mode will be described with reference to Fig. 11. Fig. 11(A) shows 6 KB aligned units formed from three 2 KB user sector data, similar to that in Fig. 10(B), and Fig. 11(B) shows the 16B un-encrypted portion 401 and the other encrypted portion 402.

[0127]

The encrypted portion 402 is divided into plaintext units of 16B each, as shown in Fig. 11(C). The first 16 byte plaintext unit is EXORed with an initial value (IV), and further is AES-encrypted and output, and 16-byte encrypted text is set. Further, this 16-byte encrypted text is EXORed with the next 16 byte plaintext unit and AES-encrypted, and a 16-byte encrypted text unit is generated. Further, this 16-byte encrypted text is EXORed with the next 16-byte plaintext unit. Thereafter the same processing is repeated, and the encrypted text unit arrangement shown in Fig. 11(D) is generated. The key in the case of AES

encryption uses the block key described with Fig. 10. Also, the initial value (IV) uses a predetermined 128-bit value which is shared between the encryption facility and the playback device.

[0128]

Thus, the encrypted data of one 6 KB Aligned Unit formed with the 16B un-encrypted portion 401 and the other 6128B encrypted portion 402 shown in Fig. 10(C) is generated.

[0129]

Next, encryption processing with a 2 KB user sector data set as the encryption processing unit will be described with reference to Fig. 12. Fig. 12(A) shows a setting with the shuffled plaintext as 2 KB user sector data.

[0130]

Encryption processing is executed using AES_ECBC, that is to say, a CBC (Cipher Block Chaining) mode of AES encryption, with one 2 KB user sector data as a processing unit, as described with reference to Fig. 11. The key to use for encryption processing is the block key (128 bits) generated by the AES key generating processing from the placement EXOR and AES encryption based on the above-described title key (128 bits), and the block key generating data (128 bits) acquired from the first 16B un-encrypted portion 411 of the 2 KB user sector data. The block key is generated using the block key generating data acquired from

the first 16B un-encrypted portion 411 of the 2 KB user sector data, and so a different key is set for each 2 KB user sector data.

[0131]

The encryption processing in AES_ECBC mode is as described with reference to Fig. 11, and as a result of the encryption processing, the encryption data of the 2 KB user sector data formed from the 16B un-encrypted portion 411 and the other 2032B encrypted portion 412 shown in Fig. 12(B) is generated.

[0132]

In the case of executing the encryption processing with 2 KB user sector data units as described with reference to Fig. 12, the chain in CBC mode is in a configuration which is completed for every 2 KB. First, the shuffle elements are set to 2KB as described with reference to Fig. 8 and so forth. Accordingly, the chain relationship in AES_ECBC mode is completed for every shuffle element. Accordingly, with the configuration performing 2 KB unit encryption, the results obtained from changing the processing order of the scrambling processing (shuffling processing) and the encryption processing are the same, and so there is the advantage of being able arbitrarily set the process order of the scramble process and the encryption process. This advantage is the same for both data recording processing and

data playback processing.

[0133]

Data configuration of a help file (MSTBL.DAT) to use in the encryption facility such as the disk plant and so forth which executes the encryption processing for deciding the process form of the encryption process in the event of data recording is shown in Fig. 13, and the syntax of this help file is shown in Fig. 14.

[0134]

The help file is set so that the type of recording data and position information is described from [UD_START_Location] through [MKB_Location], and after this, encryption processing for each sector is executed based on the flag [Encryption_Flag]. As for the data type for each Aligned Unit, differentiation between first through third sectors, and data other than AV stream data, such as Java code for example, can be distinguished, and changing the encryption processing forms based on these data types can be performed also.

[0135]

The various data has the following definitions, as shown in Fig. 14.

UD_START_Location: Physical Sector Number of start location of User Data for each Layer (Data Zone).

UD_END_Location: Physical Sector Number of end location of

User Data for each Layer (Data Zone).

CHT_Location: Physical Sector Number of CHT start location.

CHT_Offset: Start location of CHT and number of bytes until directly before Hash Value (Data to be filled in by Mastering Facility).

Content_Cert_Location: Physical Sector Number of Content Certificate start location.

Content_Cert_Offset: Start location of Content Certificate and number of bytes until directly before Content ID (Data to be filled in by Mastering Facility).

UK_Inf_Location: Physical Sector Number of title key file start location. In the event that no Unit_Key.inf is stored in that Layer, specify 0000000016.

UK_Inf_Offset: Start location of Unit_Key.inf and number of bytes until directly before Encrypted Unit Key for CPS Unit #1. In the event that no Unit_Key.inf is stored in that Layer, specify 0000000016.

Num_of_UK: Number of Unit Keys of entire Disc (= number of CPS Units).

MKB_Location: Physical Sector Number OF MKB start location. In the event that no MKB_Cert is stored in the Layer, specify 0000000016.

N: Logical Sector NUMBER OF Layer i.

Encryption_Flag: Flag for whether or not to encrypt.

Data_Type: Flag showing Type of Sector.

CPS_Unit_No: CPS Unit Number.

Clip_AV_File_No: Clip file number. Information to be used for the purpose of CHT creation.

Last_Sector_of_Clip: Flag showing last Sector of each clip (regardless of Layer).

Last_Sector of Layer: Flag showing last Sector of each clip in each Layer.

[0136]

With the example described earlier with reference to Fig. 7 and thereafter, a processing example whereby the authoring facility executes the scrambling process has been described, but next, an example whereby the disk plant (encryption facility) executes the two processes of scrambling processing and encryption processing will be described with reference to Fig. 15.

[0137]

As shown in Fig. 15, first, editing processing in the authoring facility 430 which executes the content editing processing, that is to way, the authoring process in step S271 is executed as to the content stored in the information recording medium, and the authored content 332 is generated. The authoring content is normally set as content which has been encoded with MPEG encoding or the like.

[0138]

The authoring content does not execute the scrambling

processing, but transfers this to the encryption facility (disk plant) 470. The encryption facility (disk plant) 470 selects the applicable scramble rule 451, and executes scrambling processing in step S272 based on the selected scramble rule. After scrambling processing is performed in step S272, encryption processing for the scrambled content is executed in step S273. The license entity 450 executes the administration of the MKB which is the above-described encryption key block, the media key Km is provided to the encryption facility 470 which executes the content encryption processing, the encryption facility 470 executes processing using the media key and generates the title key, and according to the methods described earlier with reference to Fig. 10 and Fig. 12, generates the block key and executes content encryption processing.

[0139]

The encryption content 452 and the scramble rule 451, which are generated by the encryption processing in step S273, are written into the information recording medium 100 with the encryption facility 470, and the information recording medium 100 is manufactured.

[0140]

Fig. 16 is a diagram showing the generating processing of the recorded data described in Fig. 15 as changes to the content data, and shows a processing example in the case of

using shuffle processing as the scrambling process. From the top layer, the diagram shows (A) plaintext before shuffling processing, (B) plaintext after shuffling processing, and (C) shuffled encrypted text. Fig. 15(A) is the data to be generated by the authoring facility, and is the content encoded by MPEG encoding or the like, that is to say, the content such as an AV stream or the like which is recorded on the information recording medium.

[0141]

Fig. 15(B) shows plaintext after the shuffling process. The content is divided into 64 KB each from the front, and is set as shuffle units for every 64 KB, and shuffling is executed for thirty-two 2 KB shuffle elements. After this, encryption processing is executed, and the shuffled encrypted text shown in Fig. 15(C) is generated. According to the present processing example, the disk plant, which is the encryption facility, executes the data generating in Fig. 15(B) and (C).

[0142]

The encryption processing can have the same settings as described earlier with reference to Fig. 10 through Fig. 12, that is to say, there is a setting using a 6 KB Aligned Unit as the encryption processing unit and a setting using a 2 KB user sector data as the encryption processing unit. With the setting using a 2 KB user sector data as the encryption

processing unit, the scrambling process and the encryption process can be reversed as to one another and the result thereof will be the same, and so processing can be performed in any arbitrary order.

[0143]

As described with reference to Fig. 7 and thereafter, the information recording medium manufacturing process of the present invention executes the scramble rule selection processing for selecting the scramble rule to apply to the content to be recorded to the information recording medium, and the scrambling processing which executes scrambling processing according to the selected scramble rule, and the processing for recording the generated scrambled content and the scramble rules selected for and applied to the content. With the scramble rule selecting process, processing is executed for selecting individual scramble rules for each recording content or each management unit in the event that there are multiple contents to be recorded to the information recording medium.

[0144]

Also, for the scramble processing, there are EXOR processing, rotation processing, and so forth, besides the shuffling processing of shuffle elements which are set as content-comprising data as described above. These processes will be described below.

[0145]

[(2-2) Exclusive-OR (EXOR) processing]

Next, a processing example using exclusive-OR (EXOR) processing as scrambling processing will be described. First, before the description of this processing example, the encoded data of an AV stream recorded onto the information recording medium, that is to say, the data configuration of an MPEG 2 transport stream data, will be described.

[0146]

Fig. 17 is a diagram showing the data configuration of an MPEG 2 transport stream data. The MPEG 2 transport stream data is set as linked data of the 6 KB Aligned Units as shown in Fig. 17(A). Each of the 6 KB Aligned Units comprise thirty-two 192-bit source packets, as shown in Fig. 17(B). The thirty-two 192-bit source packets equate to three 2 KB user sector data.

[0147]

Each of the 192-bit source packets comprise a 4-bit TP_extra header and a 188-bit transport packet as shown in Fig. 17(C). Fig. 18(A) shows the syntax of the source packet, Fig. 18(B) shows the syntax of the TP_extra header, and Fig. 19 shows the transport packet syntax.

[0148]

The processing used for applying EXOR processing as the

scrambling processing is executed as processing which EXORs a predetermined n-bit (32-bit) value with n-bit data (for example 32-bit) in a predetermined position on the transport stream data of the plaintext. The predetermined n-bit (32-bit) value is the value regulated by the scramble rule.

[0149]

The transition of the content (MPEG 2 stream data) in the case of executing scrambling processing (EXOR processing) with an authoring facility will be described with reference to Fig. 20.

[0150]

Fig. 20(A) shows data making up an MPEG 2 transport stream. With the authoring facility, the value (32-bit value Vi) which is determined based on the scramble rule is acquired, and processing to EXOR the n-bit (32-bit) value acquired from the scramble rule is executed at the position of configuration data in the predetermined MPEG 2 transport stream, and the EXOR-completed plaintext in Fig. 20(B) is generated.

[0151]

The scramble rule is for example set as the rule shown in Fig. 21. The 32-bit data of V(1) through V(n) is stored in Fig. 21, and the various V(i) values or the values calculated based on these are EXORed with the n positions of 32-bit data selected from the MPEG 2 transport stream in

order, and data rewriting is executed, and scrambling processing is performed. Now, one value, for example only V(1) can be set as the scramble rule, and the same value V(1) or a value calculated based on this can be EXORed to the n positions of 32-bit data selected from the MPEG 2 transport stream.

[0152]

In the case of performing EXOR as the scrambling processing, the scramble rule recorded onto the information recording medium has the rule shown in Fig. 21, that is to say the EXOR calculation executing value or the value to be the basis for the executing value is recorded. In the event of descrambling in the playback processing, the original data can be restored by EXORing this value or the value calculated based on this value again as data of a predetermined position.

[0153]

Returning to Fig. 20, the transition of the content (MPEG 2 stream data) in the case of executing scrambling processing (EXOR processing) with an authoring facility will continue to be described. With the authoring facility, for example the scramble rule shown in Fig. 21 is used and EXOR processing is executed, and the EXOR-completed plaintext shown in Fig. 20(B) is generated, and this data is provided to the disk plant which is the encryption facility.

[0154]

The disk plant which is the encryption facility executes encryption processing as to this received data, and generates the EXOR-completed encrypted text shown in Fig. 20(C). The encryption processing uses processing which uses the AES_ECBC mode described earlier with reference to Fig. 10 through Fig. 12.

[0155]

Thus, even if the data subjected to EXOR performed is decoded, the correct data cannot be acquired. In order to acquire the correct data, descrambling processing is necessary wherein the predetermined n-bit (32-bit) value used for EXOR is EXORed with the predetermined positions, and the original transport stream data is restored. The predetermined n-bit (32-bit) value is regulated by the scramble rule, and scramble rule deciphering with the appropriate procedures must be performed.

[0156]

In the event of using EXOR processing as the scrambling processing, as the selection configuration of the data to be processed with EXOR, either the processing in (a) or (b) as follows can be used.

(a) EXOR processing is performed with a predetermined pattern and without regard to the data content.

(b) EXOR processing is performed on specified selected

positions.

[0157]

Further, in the case of performing EXOR processing only to specified selected position as in the above (b), one of the following three positions can be selected as the EXOR use position.

(b1) a portion of the VLC wherein a slice of an I-picture is encoded (variable length run length encoded data)

(b2) a portion or all of the sequence header

(b3) a PID within a TS packet

Each of these settings examples will be described.

[0158]

(b1) a portion of the VLC wherein a slice of an I-picture is encoded (variable length run length encoded data)

The MPEG 2 encoded data is configured of GOP (Group of Pictures) data which is configured with I-, P-, and B-pictures. An I-picture is the image data to be used as a standard, and the P- and B- pictures are data configured from the difference data each from the I-picture or the like, and when the configuration of the I-picture is distorted, reproducing (decoding) the frame data contained in the GOP is difficult.

[0159]

Also the VLC wherein the slice of the I-picture is decoded is run length encoded data of the I-picture as the

backbone data, and in the event that EXOR calculations are performed using the predetermined n-bit (32-bit) value as to this VLC, replaying the original data with the decoding of the EXOR calculation processing data becomes impossible, and effective scrambling is realized.

[0160]

Even in the event that EXOR processing is performed without regard to the data content, the greater part of the transport stream is VLC data, and so there is a high probability of effectively scrambling the data. That is to say, if the processed data is played back, the correct image will not show.

[0161]

The location of the I-picture can be found with an EP map (EP_map) contained in the clip information. As shown in Fig. 22, an EP map (EP_map) 501 is data contained in the clip information.

[0162]

The detecting of the I-picture location based on the EP map will be described with reference to Fig. 23. Fig. 23(A) shows a clip AV stream, and each rectangle shows a 192-bit source packet. Each source packet has a time stamp set therein, and the playback processing time is regulated.

[0163]

Fig. 23(B) shows a detailed configuration of the source

packet No. (X1). One source packet comprises a TP_extra header and a transport packet, and the transport packet comprises various header information and I-PICH data and the like as the MPEG 2 entity data.

[0164]

The clip information shown in Fig. 23(C) contains an EP map as described above. The EP map contains the various data [PTS_EP start], [SPN_EP start], and [I_end_position_offset], as shown in the diagram. The definitions of the various data is as follows.

PTS_EP_start: a time stamp corresponding to a source packet containing a sequence header.

SPN_EP_start: a heading address of a source packet containing a sequence header.

I_end_position_offset: an offset of a source packet containing the end of the I-picture from the source packet containing a sequence header.

Fig. 23(D) shows the data relationship herein.

[0165]

In other words, as shown in Fig. 23(B), the configuration of the data contained in the source packet is regulated, and by finding the various data [PTS_EP start], [SPN_EP start], and [I_end_position_offset] as shown in Fig. 23(C) from the EP map, the I-picture locations in the source packet can be found, based on this data.

[0166]

At the time of data recording and at the time of data playback, the I-picture location is found from the EP map information, and EXOR is performed using the predetermined n-bit (32-bit) value.

[0167]

However, the configuration can be such that the EP map is not used, but rather a table is prepared which describes all of the Logical Block Addresses of the positions to be EXORed, and the scramble location is found based on this table. In this event, this table is also recorded on the information recording medium as a scramble rule. In the case of executing descrambling in the event of playback processing, the scramble (EXOR) location and value are acquired based on the scramble rule formed from this table and the EXOR value shown in Fig. 22, and EXOR processing is executed and descrambling is performed.

[0168]

The scrambling of the VLC wherein an I-picture slice is encoded, that is to say a processing example wherein EXOR calculation is executed, will be described with reference to Fig. 24. As shown in Fig. 24, the VLC wherein an I-picture slice is encoded, is sectioned by a start code showing the head location of each slice, and with the authoring facility, the value determined based on the scramble rule (32-bit

value Vi) is acquired, and EXOR processing is executed to the n-bit (32-bit) value acquired from the scramble rule to the predetermined slice location of the MPEG 2 transport stream.

[0169]

Each slice has VLC coding, and so when rewriting of a portion occurs due to the EXOR calculations, decoding (MPEG decoding) of the entire GOP corresponding to the slice becomes impossible. Thus, with the scrambling, or EXOR processing, of the VLC wherein an I-picture slice is encoded, scrambling can be effective.

[0170]

(b2) a portion or all of the sequence header

Next, an example which sets a portion or all of the sequence header as data to be EXOR calculated will be described.

[0171]

The sequence header is a header attached to the front of the GOP. The location of this sequence header can also be calculated based on the EP map described earlier. As with the above-described case, the configuration can be such that the EP map is not used, but rather a table is prepared which describes all of the Logical Block Addresses of the positions to be EXORed, and the scramble location is found based on this table. In this event, this table is also

recorded on the information recording medium as a scramble rule. In the case of executing descrambling in the event of playback processing, the scramble (EXOR) location and value are acquired based on the scramble rule formed from this table and the EXOR value shown in Fig. 22, and EXOR processing is executed and descrambling is performed.

[0172]

The sequence header has information recorded for determining the processing form of the MPEG decoding processing, and without this information the correct decoding (MPEG decoding) is impossible. Accordingly, by rewriting the values of this sequence header with EXOR calculations, data restoring can be made impossible, and so an effective scramble is realized.

[0173]

The scrambling of the sequence header, that is to say a processing example wherein EXOR calculation is executed, is shown in Fig. 25. As shown in Fig. 25, multiple 32-bit values V(i) are used for the data region containing the sequence header, and EXOR processing is executed.

[0174]

The value to be used for EXOR is acquired from the scramble rule. In other words, for example the data regulating the various 32-bit values shown in Fig. 22 is used. In the case of descrambling also, the data is

acquired and by executing EXOR processing to the same location, the original sequence header information can be acquired.

[0175]

(b3) a PID within a TS packet

Next, an example which sets a PID within a TS packet as data to be EXOR calculated will be described.

[0176]

The PID in the TS packet is 13-bit data within the transport packet (see Fig. 19). This PID data is either data contained in the transport packet, or is data for distinguishing the data type such as whether it is video data or audio data, and is incomplete data for decoding processing. Rewriting this data with EXOR calculations, makes correct decoding impossible, and so effective scrambling is realized.

[0177]

The PID location within the TS packet is regulated in advance, and can be easily found. However, even in the case of this processing example, as with the above-described example, the configuration can be such that a table is prepared which describes all of the Logical Block Addresses of the positions to be EXORed, and the scramble location is found based on this table. In this event, this table is also recorded on the information recording medium as a

scramble rule. In the case of executing descrambling in the event of playback processing, the scramble (EXOR) location and value are acquired based on the scramble rule formed from this table and the EXOR value shown in Fig. 22, and EXOR processing is executed and descrambling is performed.

[0178]

With the processing example described earlier with reference to Fig. 20, a process example wherein the authoring facility executes the EXOR calculation processing as the scrambling processing has been described, but next, an example wherein two scrambling processes which are EXOR calculation processing and encryption processing are executed in the disk plant (encryption facility) will be described with reference to Fig. 26.

[0179]

Fig. 26(A) shows data making up the MPEG 2 transport stream. The authoring facility generates the MPEG 2 transport stream as the edited content, and provides this to the disk plant which is an encryption facility.

[0180]

The disk plant which is an encryption facility acquires the value (32-bit value Vi) which is determined based on the scramble rule, and executes EXOR processing of the n-bit (32-bit) value acquired from the scramble rule at position of configuration data in the predetermined MPEG 2 transport

stream, and generates the EXOR-completed plaintext in Fig. 26(B).

[0181]

The scramble rule is set as the rule shown in Fig. 21, for example. The 32-bit data of V(1) through V(n) is stored in Fig. 21, and the various V(i) values are EXORed to the n positions of 32-bit data selected from the MPEG 2 transport stream in order, and data rewriting is executed, and scrambling processing is performed. Now, one value, for example only V(1) can be set as the scramble rule, and the same value V(1) can be EXORed sequentially to the n positions of 32-bit data selected from the MPEG 2 transport stream.

[0182]

The disk plant which is an encryption facility further executes encryption processing as to this data, and generates EXOR-completed text as shown in Fig. 26(C). The encryption processing uses the processing using AES_ECBC mode as described earlier with reference to Fig. 10 through Fig. 12.

[0183]

Thus, even if the data having EXOR performed is decoded, the correct data cannot be acquired. In order to acquire the correct data, descrambling processing is necessary wherein the predetermined n-bit (32-bit) value used for EXOR

is EXORed to the predetermined positions, and the original transport stream data is restored. The predetermined n-bit (32-bit) value is regulated by the scramble rule, and scramble rule deciphering with the appropriate procedures must be performed.

[0184]

[(2-3) Rotation processing]

Next, a processing example using rotation processing as the scrambling processing will be described.

[0185]

The processing used for rotation processing as the scrambling processing is executed as processing which executes rotation by the number of bits as regulated by the scramble rule, to the n-bit (for example 32-bit) data in a predetermined position on the transport stream data of the plaintext. The predetermined number of rotation bits is a value which is regulated by the scramble rule.

[0186]

The transition of the content (MPEG 2 stream data) in the case of executing scrambling processing (rotation processing) at an authoring facility will be described with reference to Fig. 27.

[0187]

Fig. 27(A) shows data making up an MPEG 2 transport stream. With the authoring facility, the number of rotation

bits which is determined based on the scramble rule is acquired, and rotation processing by the number of bits acquired based on the number of rotation bits acquired from the scramble rule is executed as to the comprising bits in rotation regions 611 and 612 of the predetermined MPEG 2 transport stream, and the rotated plaintext in Fig. 27(B) is generated.

[0188]

The scramble rule is set as the rule shown in Fig. 28 for example. The data of the number of rotation bits of V(1) through V(n) is stored in Fig. 28.

Using this table, the following rotation (bit exchange) is performed.

The first rotation position is bit shifted by V(1) to the left.

The second rotation position is bit shifted by V(2) to the left.

The third rotation position is bit shifted by V(3) to the left.

. . .

The nth rotation position is bit shifted by V(n) to the left.

[0189]

In the event of executing rotation processing as the scrambling process, this table is stored in the information

recording medium as the scramble rule. This table is encrypted and recorded to the disk for example so the rule is not deciphered. For all rotation positions, rotation can be performed by the same number of bits, and in this case, one shift amount [V(1)] is the only scramble rule needed for regulating. So for example, in the case of performing rotation within a 32-bit unit, the shift amount X is regulated with a setting of X, 32.

[0190]

In the event of executing rotation processing as the scrambling process, the scramble rule recorded in the information recording medium is the rule shown in Fig. 28, that is to say the data value of the number of rotation bits, is recorded. In the event of descrambling during playback processing, the original data can be restored by executing reverse rotation again based on this value.

[0191]

Returning to Fig. 27, the transition of the content (MPEG 2 stream data) in the case of executing scrambling processing (rotation processing) with an authoring facility will continue to be described. With the authoring facility, for example the scramble rule shown in Fig. 28 is used and rotation processing is executed.

[0192]

The 32-bit data at the rotation location 611 is the 32-

bit data set initially in the sequence b0 through b31, but the [b11] is shifted to the head by the rotation. In other words, 11-bit left shifting is executed. Similarly, the 32-bit data at the rotation location 612 is the 32-bit data set initially in the sequence b0 through b31, but the [b25] is shifted to the head by the rotation. In other words, 25-bit left shifting is executed. This shift amount is determined based on the scramble rule. The authoring facility executes such rotation processing based on the scramble rule, and rotated plaintext is generated as shown in Fig. 27(B), and this data is provided to the disk plant which is the encryption facility.

[0193]

The disk plant which is the encryption facility executes encryption processing as to this received data, and generates the rotated encrypted text shown in Fig. 27(C). The encryption processing uses processing which uses the AES_ECBC mode described earlier with reference to Fig. 10 through Fig. 12.

[0194]

Thus, even if the data having rotation processing performed is decoded, the correct data cannot be acquired. In order to acquire the correct data, the execution location data of the rotation process must be reverse-rotated correctly in the amount of the number of executed rotation

bits, and with this processing, descrambling can be performed. The number of rotation bits is regulated by the scramble rule, and scramble rule deciphering with the appropriate procedures must be performed.

[0195]

In the event of using rotation processing as the scrambling processing, either the processing in (a) or (b) as follows can be used, as with the position of the data to be processed with EXOR.

(a) Rotation processing is performed with a predetermined pattern and without regard to the data content.

(b) Rotation processing is performed at specified selected positions only.

Further, in the case of performing rotation processing only at specified selected position as in the above (b), one of the following three positions can be selected as the rotation position.

(b1) a portion of the VLC wherein a slice of an I-picture is encoded (variable length run length encoded data)

(b2) a portion or all of the sequence header

(b3) a PID within a TS packet

[0196]

With the processing example described with reference to Fig. 27, a process example wherein the authoring facility executes the rotation processing as the scrambling

processing has been described, but next, an example wherein two scrambling processes which are rotation processing and encryption processing are executed in the disk plant (encryption facility) will be described with reference to Fig. 29.

[0197]

Fig. 29(A) shows data making up the MPEG 2 transport stream. The authoring facility generates the MPEG 2 transport stream as the edited content, and provides this to the disk plant which is an encryption facility.

[0198]

The disk plant which is an encryption facility acquires the number of rotation bits which is determined based on the scramble rule, and executes rotation processing in the number of rotation bits acquired from the scramble rule at the position of configuration data in the predetermined MPEG 2 transport stream, and generates the rotated plaintext in Fig. 29(B).

[0199]

With the 32-bit data in the rotation region 621, [b11] is shifted to the head by the rotation. In other words, 11-bit left shifting is executed. Similarly, with the 32-bit data at the rotation region 622, [b25] is shifted to the head by the rotation. In other words, 25-bit left shifting is executed. This shift amount is determined based on the

scramble rule. The scramble rule is set as the rule shown in Fig. 28 for example. The disk plant which is the encryption facility executes encryption processing further as to this data, and generates the rotated encrypted text shown in Fig. 29(C). The encryption processing uses processing which uses the AES_ECBC mode described earlier with reference to Fig. 10 through Fig. 12.

[0200]

Thus, even if the data subjected to rotation is decoded, the correct data cannot be acquired. In order to acquire the correct data, the execution location data of the rotation process must be reverse-rotated correctly in the amount of the number of executed rotation bits, and with this processing, descrambling can be performed. The number of rotation bits is regulated by the scramble rule, and scramble rule deciphering with the appropriate procedures must be performed.

[0201]

Now, up to this point, shuffling processing, EXOR processing, and rotation processing have been described as three types of scrambling processing forms, but these scrambling processes can be combined and used.

[0202]

Also, as the data used for scrambling processing, with the EXOR processing and rotation processing, settings

examples which have data containing at least one of the following have been described.

(1) a portion of the I-picture slice encoded data contained in the MPEG encoded data

(2) a portion of the sequence header

(3) PID data which has information recorded which is data type specific within the transport stream packet

However, in the same way, the shuffling processing also can be performed with data containing one of the above (1) through (3) being selected.

[0203]

[3. Configuration examples of the information processing device]

Next, examples of the information processing device which performs playback processing or recording processing of the content having performed the above-described scrambling processes will be described with reference to Fig. 30.

[0204]

The information processing device 800 drives the information recording medium 891, and comprises a drive 890 for performing input and output of the data recording playback signal, a CPU 870 for executing data processing according to the various programs, ROM 860 serving as a storage region for programs, parameters, and the like,

memory 880, an input/output I/F 810 for inputting and outputting a digital signal, an input/output I/F 840 which inputs and outputs an analog signal and which has an A/D, D/A converter 841, an MPEG codec 830 for executing encoding and decoding processing for MPEG data, a TS/PS processing means 820 for executing TS (Transport Stream)/PS (Program Stream) processing, an encryption processing means 850 for executing various encryption processing, and a scrambling processing means 855 for executing scrambling processing or descrambling processing, with a bus 801 being connected to each block.

[0205]

First, the operation at the time of data recording will be described. As data performing recording, the two cases of digital signal input and analog signal input can be considered.

[0206]

In the case of digital signals, the signal is input from the digital signal input/output I/F 810, and converted to a data format for saving by the CPU 870 and the TS/PS processing means 820, and data conversion processing to for example an MPEG 2 format is performed by the MPEG codec 830, and scrambling processing according to the predetermined scramble rule is executed with the scrambling processing means 855. The scramble rule is stored for example in the

memory 880. The form of the scrambling processing to be performed is the applicable one of shuffling processing, EXOR processing, or rotation processing, as described above. In the case of using any one of shuffling processing, EXOR processing, or rotation processing, rules which differ for each content or content management unit can be used.

[0207]

Also, the configuration can be such that rather than using one method of scrambling processing among the shuffling processing, EXOR processing, or rotation processing, a multiple of the shuffling processing, EXOR processing, or rotation processing can be combined and used.

[0208]

The data subjected to scrambling is then subjected to encryption processing by the encryption processing means 850. The encryption processing is executed as processing using for example AES_ECBC mode, as described with reference to Fig. 10 through Fig. 12. The encryption processing units using AES_ECBC mode can be 2 KB unit, 6 KB units, or other various settings. The data on which encryption processing is performed by the encryption processing means 850 is saved to the information recording medium 891.

[0209]

In the case of analog signals, the analog signal input to the input/output I/F 840 is converted to a digital signal

by the A/D converter 841, and is converted to the codec to be used at time of recording by the MPEG codec 830. After this, the data is converted to AV multiplexed data, which is a recorded data format, by the TS/PS processing means 820, and as needed, scrambling processing by the scrambling processing means 855 and encoding processing by the encoding processing means 850 are performed, and the data is saved to the recording medium 891.

[0210]

Next, processing in the event of performing data playback from the information recording medium will be described. For example, in the event that playback of AV stream data, which is formed of MPEG-TS data, is to be performed, when the data which is read out from the information recording medium 891 in the drive 890 is identified as a content management unit, the acquiring processing of the unit key corresponding to the content management unit is executed, and based on the acquired unit key, encryption is solved with the encryption processing means 850, and after this, descrambling processing is executed.

[0211]

In the event of descrambling processing, the scramble rule is read out from the information recording medium 891, and the scramble rule used for the content to be played back

must be deciphered. For example, in the case that content scrambling is executed as shuffling, the scramble rule with the settings for the shuffle element sequence shown in Fig. 9 (A) is acquired, if execution is with EXOR, the scramble rule with the settings for the EXOR value shown in Fig. 21 is acquired, and if execution is with rotation, the scramble rule with the settings for the number or rotation (shift) bits is acquired, and based on these acquired rules the descrambling is executed. As described above, the analyzing of the scramble rules and the descrambling processing are executed as secure data processing. Specifically, the scramble rules stored in the information recording medium for example are recorded with a Java secure code, and the scramble rule deciphering and descrambling processing are executed with Java VM (virtual machine) set in the information processing device which executes content playback.

[0212]

The content data on which descrambling is performed is then divided into various data such as Video, Audio, or Captions, by the TS (Transport Stream)/PS (Program Stream) processing means 820. Further, the digital data decrypted with the MPEG codec 830 is converted to an analog signal by the D/A converter 841 within the input/output I/F 840. Also in the event of performing digital output, the MPEG-TS data

is output as digital data through the input/output I/F 810. The output in this case is performed as to a digital interface such as IEEE 1394 or Ethernet cable or wireless LAN. In the event of corresponding to the network connection function, the input/output I/F 810 provides functionality for network connections. Also, in the event of converting and outputting data to a format receivable by an output device within the playback device, rate conversion and codec conversion processing is added with the MPEG codec 830 as to the Video, Audio, and Captions separated during the TS/PS processing means 820, and the data having been multiplexed again to MPEG-TS or MPEG-PS with the TS/PS processing means 820 is output from the digital input/output I/F 810. Also, conversion can be made to a codec other than MPEG, or to a multiplexed file using the CPU 870, for output from the digital input/output I/F 810.

[0213]

The program which executes playback processing and recording processing is stored in the ROM 860, and during the program execution processing, the memory 880 is used as needed for storing parameters and data, and as a work area. In Fig. 30, the device configuration is described as being capable of data recording and playback, but devices with playback functionality only, or with recording functionality only can be configured, and the present invention can be

applicable to such devices also.

[0214]

The present invention has been described in detail above with reference to specified embodiments. However, it should be understood that various changes and modifications to the embodiments could be made by one skilled in the art without departing from the spirit or scope of the invention. In other words, the present invention is disclosed in the form of examples, and should not be given a limited interpretation. In order to determine the scope of the present invention, the appended claims should be referred to.

[0215]

The series of processing described in the description herein can be executed with a configuration of hardware, or software, or a combination thereof. In the case of executing processing with software, a program storing the processing sequence can be installed into the memory of the computer which has built-in dedicated hardware, with executing being performed, or a program can be installed into a general-use computer wherein various types of processing can be executed.

[0216]

For example, the program can be recorded in advance on a hard disk or in ROM (Read Only Memory) serving as the recording medium. Alternatively, the program can be stored

(recorded) temporarily or permanently onto a removable recording medium such as a flexible disk, CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) disk, DVD (Digital Versatile Disc), magnetic disk, or semiconductor memory. Such removable recording media can be provided as so-called packaged software.

[0217]

Other installing the program on the computer from the above-described removable recording media, the program can be wirelessly transferred to the computer from a download site, or can be transferred by wire to the computer via a network such as a LAN (Local Area Network) or the Internet, and the computer can receive the program transferred in such a manner and install the program onto a recording medium such as an internal hard disk.

[0218]

The various processing described in the description herein does not need to be executed chronologically according to the description, and can be executed in parallel or individually according to the processing capability of the device to execute the processing, or as needed. Also, system as used in the present description refers to a logical group of multiple devices, and is not limited to the various configurations being within one enclosed unit.

Industrial Applicability

[0219]

As described above, according to the present invention, scrambling processing forms with various differing forms are set, rather than setting uniform processing for scrambling processing of the various content as requested by the usage management system such as copyright management, and scrambling processing is executed with a form being selected for each content or each management unit from a large number of scrambling processing forms, and therefore, if by chance there is an event wherein scrambling for a given content is unauthorizedly decoded and the content is leaked, the content which has a scrambling process with a different scrambling form cannot be descrambled, and so leakage of content can be kept to a minimum.

[0220]

With the configuration according to the present invention, scrambling processes such as shuffling processing, EXOR processing, and rotation processing are executed, and with shuffling processing, various shuffle forms are specified as the scramble rules, and with EXOR processing, values applicable to EXOR are specified as the scramble rules, and with rotation processing, the rotation shift amounts are specified as the scramble rules. For example,

in the case of using 32 shuffle elements with shuffling processing, 32! different shuffle forms, that is to say, scramble rules, can be specified. Also, with EXOR, the values applicable to EXOR, and with rotation processing, the various values of the shift amount, can be set, and so a large number of scramble rules can be set, and a configuration is realized wherein scrambling of each content based on the rules selected from this large number of scramble rules is performed, and based on the leakage of specified scramble rules, leakage of a large amount of content can be prevented.